Information Security:
Raising Awareness

May 2000

Submitted to:
The Public Sector Chief Information Officers' Council
by the Subcommittee on Information Protection

Prepared by:
Bruce Hunter, BEng, MEng
Government of Canada PKI Secretariat
Chief Information Officer Branch
Treasury Board of Canada Secretariat

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/1/2000	Report 5/1/2000

4. TITLE AND SUBTITLE
Information Security: Raising Awareness

5. FUNDING NUMBERS

6. AUTHOR(S)
Bruce Hunter

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Government of Canada PKI Secretariat

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

As is taking place in all technically advanced nations today, federal, provincial and municipal governments in Canada are rapidly implementing new information technology infrastructures, new managerial and operational processes, and new innovative methods of delivering services to citizens electronically. The rapid advances in technology are enabling the reshaping and reengineering of governments, improving efficiency and effectiveness in ways that could have only been imagined just a few years ago. In this very exciting and challenging "information revolution", the importance of Information Security is rapidly coming into focus. This focus has been rapidly sharpened by recent events such as the troubling denial of service attacks that halted the operations of some of the largest and most advanced electronic commerce enterprises in the United States in February 2000

14. SUBJECT TERMS
IATAC Collection, information security, hacking, viruses, trojan horses

15. NUMBER OF PAGES
53

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The aim of this paper is ***to help raise awareness of and commitment to information security*** in the dynamic context of the emerging Internet economy.

As is taking place in all technically advanced nations today, federal, provincial and municipal governments in Canada are rapidly implementing new information technology infrastructures, new managerial and operational processes, and new innovative methods of delivering services to citizens electronically. The rapid advances in technology are enabling the reshaping and reengineering of governments, improving efficiency and effectiveness in ways that could have only been imagined just a few years ago. In this very exciting and challenging "information revolution", the importance of Information Security is rapidly coming into focus. This focus has been rapidly sharpened by recent events such as the troubling denial of service attacks that halted the operations of some of the largest and most advanced electronic commerce enterprises in the United States in February 2000.

Security has been a technically challenging problem with computers almost from the first instances of their operational use. Networking brought greater security challenges and the advent of the "network of networks" we refer to as the Internet is bringing even greater challenges. Provision of government services over ***the Internet has become an imperative*** in the new Information Age. When governments use the Internet for service delivery, however, ***security and privacy*** are fundamental requirements. What makes security such an issue today relates not only to the inherent technical challenges, but also to the fundamental and rapid changes in the way governments are doing business, the information infrastructures involved in this change, and the commensurate rapid rise in our dependency on these infrastructures. In simple terms, governments are now dependent on information systems to the extent that disruptions or malfunctions could mean that business functions cease.

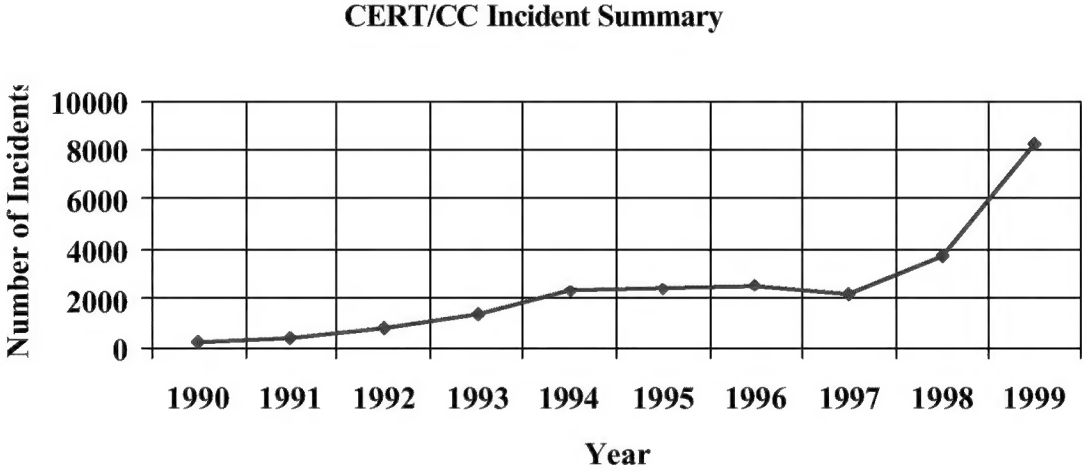
Information Security should be a fundamental part of IM/IT management. Security management involves managing risks and practising ***an appropriate standard of care.*** This task cannot be achieved by CIOs alone. Business managers, information systems specialists, and security practitioners must collaborate effectively to achieve a balanced solution. In particular, it important that the business managers be involved in the process and that security is seen as a ***business issue***. Involvement of the business managers will provide a better understanding of the trade-offs required in order to achieve a balanced approach. Security should be viewed as an enabler for change and as a necessary component of a business process.

Risk management is at the heart of information security. A risk assessment should be a fundamental part of the business development process. Part of the risk management challenge is the fact that information systems are changing quickly and, at the same time, security risks also change very quickly as new threats, vulnerabilities and attack tools are introduced. As a consequence, a static risk assessment process is no longer sufficient. Risk management must now be designed to ***a continuous process that reacts quickly to***

changes. To accomplish this, risk management should include elements of real-time assessment and response.

Awareness implies understanding risks. Internet threats and vulnerabilities are real. In simple terms the number of vulnerabilities continues to rise, while hacker tools are becoming more powerful and easier to use. At the same time, prevention is much more difficult because the technology changes rapidly. The Internet is a very attractive target for attackers. Internet attacks are easy to do, difficult to detect, hard to trace, and the risk of getting caught is low.

The alarming increase in the number of Internet security incidents demonstrates that the risks are real. Numerous sources such as the Computer Security Institute, the United States National Information Protection Center, and the CERT® Coordination Center (CERT/CC) all report a significant growth in the number of security incidents. This is reflected in the chart below. To the extent that such data is available, this paper also presents some of the security incidents and statistics from Canadian sources.



If our information systems are indeed at risk, what should be done? This paper outlines some of the fundamental security practices that governments should apply. Although not foolproof, these practises ***can drastically reduce the risk***. Implementing ***sound security policies, risk management, standards and best practises, and technological safeguards will greatly help reduce the overall risk*** exposure while demonstrating an appropriate standard of care. These practises include security management, security policies and best practices, implementation of a layered security architecture, and real-time incident detection and response. The goal of a layered security architecture is to define a set of technical safeguards and standards to provide a consistent and complete security posture. The architecture should define the common security infrastructure, a set of common solutions and standards that can be applied across organizations, and a range of technical safeguards required to support business processes. These measures, if carefully implemented, can achieve the secure environment necessary to obtain the trust and confidence of Canadians.

Much more work remains to be done. Particular emphasis is being placed on protecting Canada's critical infrastructures. The federal government recently established an interdepartmental Critical Infrastructure Protection Task Force to address this challenge. In addition, a national focus is required to develop national security infrastructures such as a national information protection coordination center and Public Key Infrastructure. These elements will require partnerships between governments and the private sector in order to achieve the ultimate goal of a secure national information infrastructure.

1. INTRODUCTION

As Canada moves into the Information Age, governments are revolutionizing the way they operate and are moving quickly to provide government services on line. The global trend toward interconnectedness and the dramatic rise of Internet use, electronic service delivery and e-government will dramatically impact government operations that rely on a complex system of networks and computers.

Although governments have relied on computers for years, there is an explosion in the use of electronic data and networked computer systems to meet the demands for e-commerce and e-government. Doing business via the public Internet is quick, easy and inexpensive. There are compelling reasons for businesses and governments to conduct business via the Internet to ensure that Canada remains competitive. Virtually all researchers predict huge growths in e-commerce and e-business over the next few years, and e-government is growing rapidly. The federal government has made Government On Line a priority and plans to provide all government services electronically by 2004. Many provinces are developing similar plans.

Today, information, systems, and networks are pervasive and ubiquitous. Many of the centralized system and network control elements have virtually collapsed with the availability of inexpensive, distributed, and remote computing with extensive interconnectivity. The information technology and communications infrastructure has been cobbled together in one of the most accelerated technological advances ever experienced in human history. It is not built to, or operated by, the kind of overarching guidance and standards applied to any other critical infrastructure. Yet, this new and fragile infrastructure is being used to support critical infrastructures and is the foundation for the "new economy". It is susceptible to abuse, misuse and denial of essential services.

Paper trails are a disappearing relic because information typically exists in electronic form today. Even personal identifiers, or "signatures" are losing the paper and ink elements that have for centuries been the basis for trust, accountability, and controls.

To be useful information must be accessible, and this very accessibility puts it at risk. Connectivity makes information available when and where it is needed, and is the nature of doing business today. Because governments will be linked via the Internet to other governments, partners, business, and citizens, they will also be connected to virtually anyone in the world. Connectivity exposes information to risks outside each organization's control.

Governments have become increasingly dependent on information systems to support operations. Although advances in information technology improve efficiencies and services, they also expose governments to greater risks. Risk factors are growing exponentially as governments move critical functions online. The Internet is a public collection of computer networks, and hooking government computers to it creates

multiple potential entry points for cyber attacks. Interconnected systems become vulnerable to anonymous intrusions from remote locations around the world.

Competitive pressures are intense. E-commerce is growing exponentially. Meanwhile, globally there are millions of technical experts capable of launching successful and economically devastating cyber attacks for less than the cost of a used car and a little time.

The benefits of this "Information Revolution" are enormous, including global reach, better client relationships, improved services, and more efficient operations. Canada's competitiveness is dependent on adopting advancements in information technology. These advancements introduce new challenges. First and foremost is privacy and security—protecting the information infrastructures and the information of governments, as well as businesses and citizens. Governments must protect both government and citizen information from exposure and tampering, protect the privacy of citizens, and protect themselves against network outages and "denial of service" attacks. Governments must earn and maintain citizens' trust, and they need to stay open for business. Perhaps more importantly, governments need to secure the systems and information that are at the ***center*** of their existence.

Information security is a complex issue that has traditionally been treated as either a technical or a security policy problem. Often those who understand the problem have not translated the threat into business terms understood by senior decision-makers or the problems have not have received the attention they deserved. As a result, information security usually was not seen as a priority requirement that needed to be addressed in order to support the business drivers of the organization. Information security now more than ever is a fundamental ***business issue***, rather than strictly a security issue. Information security is an integral part of and an enabler for new businesses processes and services. Within governments, the business community must therefore be directly involved in the inevitable trade-offs between security and business objectives.

2. AIM

The aim of this report is to provide a snapshot of the threats and vulnerabilities to government information systems, to provide a common understanding of the information protection problem, and to improve the overall awareness of and commitment to information security.

The Subcommittee on Information Protection prepared this report for the Public Sector CIO Council. This report is intended to assist CIOs in assuring the protection of information within their jurisdictions.

3. SCOPE

This document focuses primarily on ***Internet-related security issues***. The fundamental change facing government security is the provision of on-line services, where use of the

Internet is an imperative. The associated privacy and security issues are of concern to all Canadians.

The first part of this report highlights the threats and vulnerabilities associated with connecting to the Internet. The second part identifies security practices that, although not foolproof, can drastically reduce the risk. These measures, carefully applied, can achieve the trusted environment necessary to obtain the trust and confidence of Canadians.

Since this report focuses on the Internet, some aspects of security, although equally important, are not emphasized. In particular, this report does not focus on the insider threat, which is still a major source of security incidents, because the biggest change facing governments is the move to provide services over the Internet. Similarly, common safeguards such as physical and personnel security are not emphasized.

The aim of this report is to promote security awareness for government and does not address any unique requirements associated with the private sector. Secure awareness is equally important in the private sector to support the growth of e-commerce and to protect critical infrastructures, most of which are owned and operated by the private sector. Most of the security threats and vulnerabilities identified in this report are general in nature and also apply to the private sector. However, there are dramatically different business requirements and pressures in the private sector that must also be considered. More work is required for governments to work in partnership with private industry to address the overall security requirements of the national information infrastructure.

This report also does not address the problem of the current shortage of skilled information systems security personnel. The Subcommittee on Information Protection has identified numerous sources of security training and continues to promote development of training and education curricula. Fundamental improvements in the awareness and priority of information protection are needed to provide the impetus to further develop security training and education programs in Canada. In addition to the recommendations provided in this report, related skills development will require an on-going effort.

4. RISK MANAGEMENT

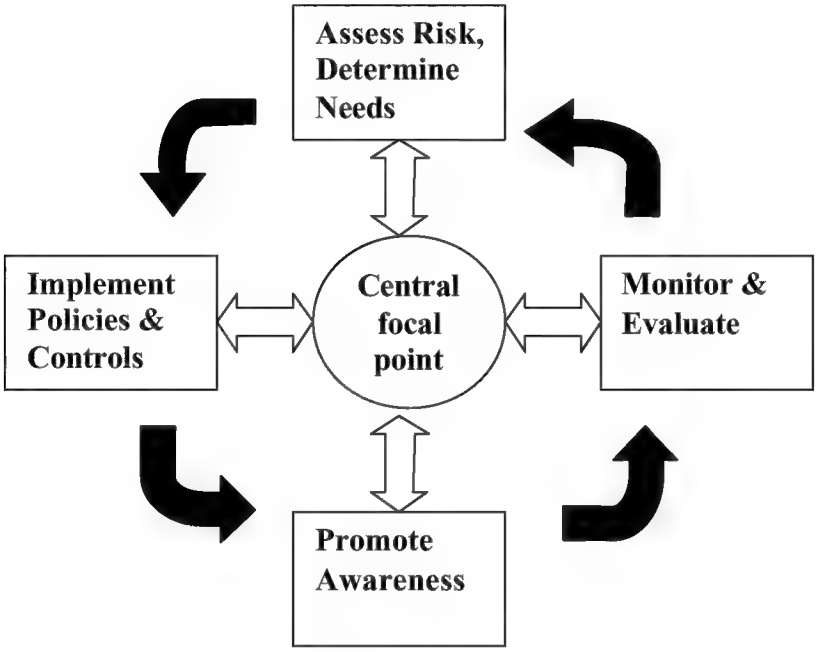
The principle of ***risk management is at the heart of information security***. Security management should follow a risk management cycle such as the one below. This model is described in the US General Accounting Office report on Information Security Management[1] and is based on common risk management principles applied by leading organizations. The five risk management principles described in the GAO report are:

> (1) Determine needs based on an assessment of information security risks in terms of the impact on business operations;
>
> (2) Establish a central management focal point to ensure that weaknesses in one organizational unit do not place the entire organization's information assets at risk;

(3) Implement appropriate policies and related controls;

(4) Promote awareness to continually educate both users and managers on risks and related policies; and

(5) Monitor and evaluate the effectiveness of policies and controls.



Risk Management Cycle

The paper focuses on the awareness component of the risk management cycle.

Awareness is an essential element of the risk management cycle and information security requires attention at all levels. Security awareness should therefore be aimed at managers, users, and information system practitioners. Awareness and understanding is essential to implement information security policies and to ensure that related controls are working properly. Managers, users, and others with access to information resources cannot be expected to comply with policies they are unaware of or do not understand. Similarly, if they are not aware of the risks associated with their information resources they may not understand the need for and support compliance with policies designed to reduce risk.

A significant challenge of risk management is the fact that the security risks change very quickly on the Internet because new vulnerabilities and attack tools are continually being identified. As a consequence a static risk assessment process is no longer sufficient. The

risk management process must now be designed to react quickly and therefore should include elements of real-time assessment and response.

Awareness implies understanding risks. The next section provides a description of the threats and vulnerabilities to Canada's information systems.

5. UNDERSTANDING THE RISKS

5.1. Threat Agents

Computer threat agents, those who initiate computer attacks, can be broken down loosely into the following areas:

(1) **Hackers**. The term "hacker" is often misused and typically refers to someone who exploits technology for its own sake. Hackers exist in various guises, from the simple and automated to the highly disguised and sophisticated. "Script kiddies" are at the low end of the scale and are the source of most attacks. They are usually teenagers who acquire some "cracking tools" on the Internet and are keen to use them. The minimum skill-set needed to be a "script-kiddy" is simply the ability to read and follow directions. Virus-writing code and exploit scripts are common, and many are automated. These "kiddies" can be dangerous. Typically "script-kiddies" deface web sites; however some believe that they are also responsible for more serious attacks such as the recent major denial of service incidents. The skills required to be a true hacker are not at all rare - similar to those required for a knowledgeable system administrator. There is also a group of highly skilled hacker "élite". In the realm of hackers, there are three types. The "black hats" are criminals who break into computer systems for malicious reasons, while the "white hats" are purists who are quick to point out that there is a code of hacker ethics that precludes illegal activity. (The term "white hat" is an oxymoron and ethical hacking can only be done by security professionals.) The "grey hats" exist in between: they write programs that reveal security holes in computer systems and post them publicly on the Internet, allegedly to draw attention to the flaws. Some call themselves "hacktivists" and claim they write programs to practice a sort of civil disobedience in cyberspace in order to bring attention to a social cause or effect political change. In addition, some companies that advocate an open approach to raise security issues openly provide cracking tools and identify new security vulnerabilities. For example, LOpht Heavy Industries offers via its website a powerful password cracking tool that also captures passwords on a network.

(2) **Insiders**. Insiders are a common source of attack that can be particularly dangerous because they often have privileges and direct access to computer systems, and are difficult to detect. Employees, disgruntled or otherwise, break into internal computer systems to find information, cause disruptions, destroy or modify data, or commit fraud. It should be noted that, although the

emphasis in this paper is placed on external Internet-based threats, the security measures described later in this report address both internal and external threats.

(3) **Non-Criminal/Accidental Threats**. There are also non-criminal threats to information such as the inadvertent sending or releasing sensitive information to the wrong party, failure to implement preventive measures correctly, errors made by users or system administrators etc.

(4) **White Collar Crime**. The lure of big, fast-money in virtual commerce as financial and business sectors move to the Internet attracts white-collar crime. Such types of crimes are rarely reported for fear of highlighting a company's own negligence and resulting in bad publicity. For example, the press has reported rumours that the financial sector has been subject to attacks but little information is released. Potential exploits include credit card fraud, stock fraud, and stealing company secrets. The Internet has become an extraordinarily efficient and cheap method of conducting stock frauds and Internet stock scams. Attackers can break into a publicly traded company's website and post a false notice to boost the stock of a competitor or can post fake press releases announcing a merger. There is particular concern about "momentum" sites, where investors are urged to buy a certain stock at a certain time in a bid to build momentum to drive its price higher. There are also "cybersmears," in which negative news about a company is disseminated on the Internet to drive down its stock price to benefit short sellers. It is also common for skilled hackers to attack competitors in search of intellectual property. The present era of "dot-com millionaires and IPO frenzies" and the perceived ease of starting a business on the Web has the potential of generating a tremendous amount of white collar crime.

(5) **Espionage**. This includes industrial, economic, or military espionage. Industrial espionage involves breaking into computers to steal, for example, research and development secrets. Economic espionage concerns intelligence activity aimed at the acquisition of sensitive information such as financial, trade, economic policy, proprietary economic information, or critical technologies. Military espionage concerns foreign intelligence activity aimed at national defence information.

(6) **Cyberterrorism**. Cyberterrorism includes those attacks intended to terrorize and influence the target population, or to influence governments by intimidation or coercion. These threats transcend national boundaries. The low financial barrier, broad accessibility, and ease of use of information technology means that the threat can come from a wide range of sources with varying profiles. It is, therefore, difficult to isolate the source of the threat or the high risk organizations.

5.2. The Nature of Internet Security

The Report of the Special Senate Committee on Security and Intelligence[2] in January 1999 highlighted the issues related to Information Protection. The report states that Canada has become an information intensive society and economy. These advanced technologies have also increased our vulnerability to potential terrorist disruption. Not surprisingly, the rapid advances in interconnections and information technology create a huge challenge in protecting the systems from intrusions and perhaps even sabotage.

The testimony of the director of the Software Engineering Institute (SEI) of Carnegie Mellon University provides a good overview of the state of Internet security[3]. The SEI is the home of the CERT® Coordination Center (CERT/CC). The CERT/CC was established more than eleven years ago, after an Internet "worm" stopped 10% of the computers connected to the Internet. Its charter was to work with the Internet community to respond to computer security events, raise awareness of computer security issues, and prevent security breaches. The CERT/CC testimony states that the following factors have lead to the current state of Internet security:

(1) Due to the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication and it is growing at an amazing rate.

(2) As the technology is being distributed, so is the management of that technology. In these cases, system administration and management often become the responsibility of people who do not have the training, skill, resources, or interest needed to operate their systems securely.

(3) Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.

(4) The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and web sites result in vulnerabilities that intruders can exploit.

(5) When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so the maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

(6) As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. There are no "silver bullet" solutions, and single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.

(7) There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities and continues to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until customers demand products that are more secure, the situation is unlikely to change.

(8) Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

Completely securing the Internet is impossible. A detailed step by step checklist for Internet security cannot exist because vulnerabilities and attacks are constantly changing. Security measures that are appropriate for well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. The Internet has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. The Internet was not originally designed with security in mind - it was designed to be "open" and cannot be administered by a central authority. The Internet was definitely never designed to be such a vital part of the economy. Furthermore, security issues are not well understood and, until recently, were not given high priority by software developers, vendors, network managers, or consumers.

The next section describes some specific Internet threats and vulnerabilities.

5.3. Internet Threats and Vulnerabilities

Hackers find and attack the weakest and most easily exploitable point of a network. The web site is usually the most exposed doorway, and the favourite target for cyber attacks. Web sites and their internal computers are usually protected with firewalls - a combination software/hardware system designed to lock out intruders. However, a poorly configured firewall can be just as bad as no firewall and could give a false sense of security. Firewalls, by design, must open some doors to permit legitimate traffic to

flow between the internal and external networks. If this is not done correctly the door can be left wide open. At the same time, new exploitation software is making the task of getting past firewalls much easier. Public web sites have programs that will do everything for the prospective attacker: find a vulnerable web site, find a way in, and give access. It's not nearly as difficult as it used to be.

Sensitive computers are normally not connected directly to the Internet and are usually protected by safeguards. However, there is usually a weak link in the chain. For example, if a government is connected to Vendor A, and Vendor A to Vendor B (and so on), somewhere in the chain there is likely a vulnerability due to the widely interconnected networks, technological dependence and complex software. Although direct attacks on sensitive systems may be unlikely, if a network has a connection elsewhere, then it may only require one vulnerability to be the weak link in the chain.

Another factor fuelling the risk is free online distribution of easy to use attack tools, which make it easy for people who don't even know computer programming to launch attacks. Intruder tools and scripted attacks are becoming increasingly sophisticated, increasingly user friendly and widely available. Developers of intruder programs package their tools into user-friendly forms and distribute them freely on the Internet. As a result, even unsophisticated intruders can use them. For example, hackers use Internet "scanner" programs to probe thousands of computers looking for openings. They download software to crack weak passwords and "trojan horses" such as "Back Orifice". For the first time, intruders are developing techniques to harness the power of large numbers of vulnerable systems on the Internet. Using these so-called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks.

Today the life cycle of a typical threat-vulnerability interaction on the Internet follows a number of predicable steps from time a new vulnerability is identified to the time when it is widely exploited by automated tools:

(1) a vulnerability is discovered or postulated and discussed in Internet news-groups, among hackers, etc;

(2) an enterprising individual or group of individuals releases code and/or a basic tool to exploit the vulnerability;

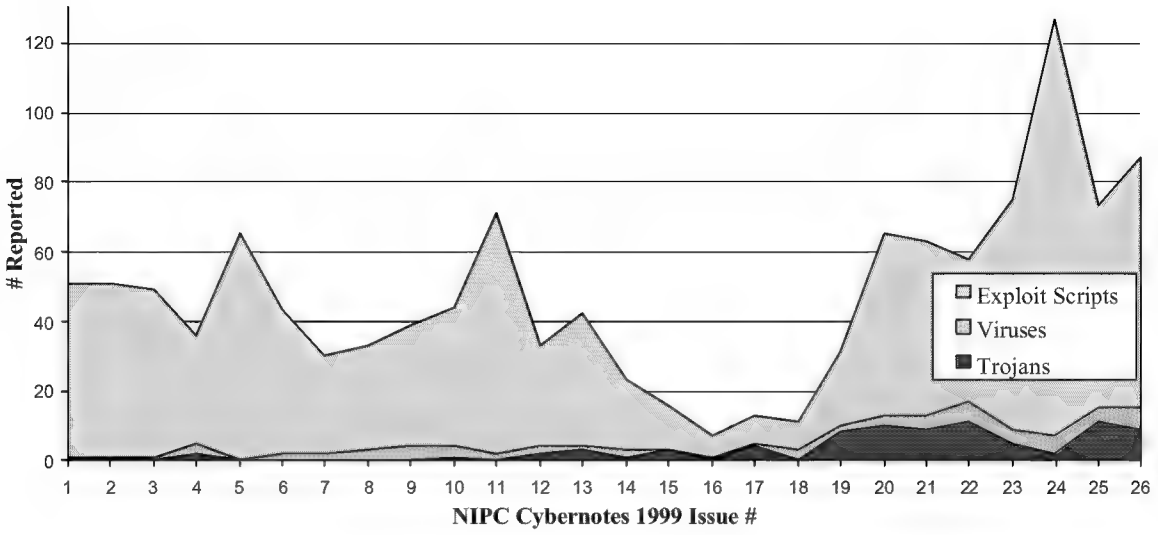
(3) some exploratory intrusion attempts are made by hackers using the crude tool;

(4) after a very short period of time the crude tool is refined into a much more advanced and easy to use exploit tool and released on the Internet;

(5) the new tool quickly proliferates and is used to search for and exploit the vulnerability across the net.

The following chart illustrates the number of new threats reported by the US National Information Protection Center (NIPC) in its bi-weekly report. The threats are divided into exploit scripts, trojans, and viruses.

Threats Reported in NIPC *Cybernotes*



For the reasons cited above, both the number and the dangers of Internet security vulnerabilities are extensive and continue to outpace our abilities to defend against them. New security vulnerabilities are reported on a routine basis by many organizations including the following:

(1) CERT® Coordination Center at http://www.cert.org publishes advisories, vulnerability notes, and incident notes. The CERT/CC also publishes quarterly summaries that draw attention to noteworthy incidents and vulnerabilities;

(2) Mitre Corporation is composing a Common Vulnerabilities and Exposures (CVE) list at http://cve.mitre.org (CVE aims to standardize the names for all publicly known vulnerabilities and security exposures to make it easier to share data across separate vulnerability databases and security tools);

(3) US Government organizations such as the Federal Computer Incident Response Capability (FedCIRC) at http://www.fedcirc.gov and the National Information Protection Center (NIPC) at http://www.nipc.gov regularly issue advisories and notices. A particularly good source of vulnerabilities is the NIPC CyberNotes that is published every two weeks by the NIPC to provide information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and best practices. For the 2 week period 14-26 Jan 00, CyberNotes published 28 new software holes, 12 of which were high risk (can gain root access), and 39 new exploit scripts, 6 of which have published no workarounds or fixes;

(4) CanCERT™ at www.cancert.ca is a privately operated incident response team in Canada that collects and disseminates information related to networked computer threats, vulnerabilities, incidents and incident responses. CanCERT™ provides information shared on a global basis through the Forum of Incident Response and Security Teams (FIRST) at http://www.first.org;

(5) Private organizations and security companies maintain lists such as the Shake Vulnerabilities Database at http://www.shake.net and ISS at http://xforce.iss.net;

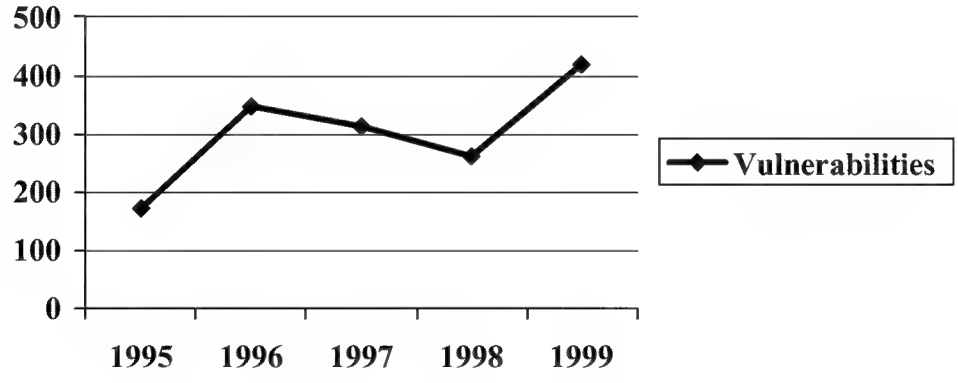
(6) SANS Institute at http://www.sans.org publishes vulnerabilities in its Security Digest; and

(7) Product specific vulnerabilities are provided at Bugtraq lists such as NTBugtraq at http://ntbugtraq.ntadvice.com.

A quick glance at these extensive lists of vulnerabilities highlights the difficulty of keeping up. There are simply too many holes to plug. Vendors continue to release software with numerous vulnerabilities and struggle to address the problem with frequent patches. A common problem is that vulnerabilities often exist because software has not been kept up to date with newer versions and patches. Systems administrators often do not have the resources and management support to keep systems patched so that vulnerabilities are fixed before they are exploited.

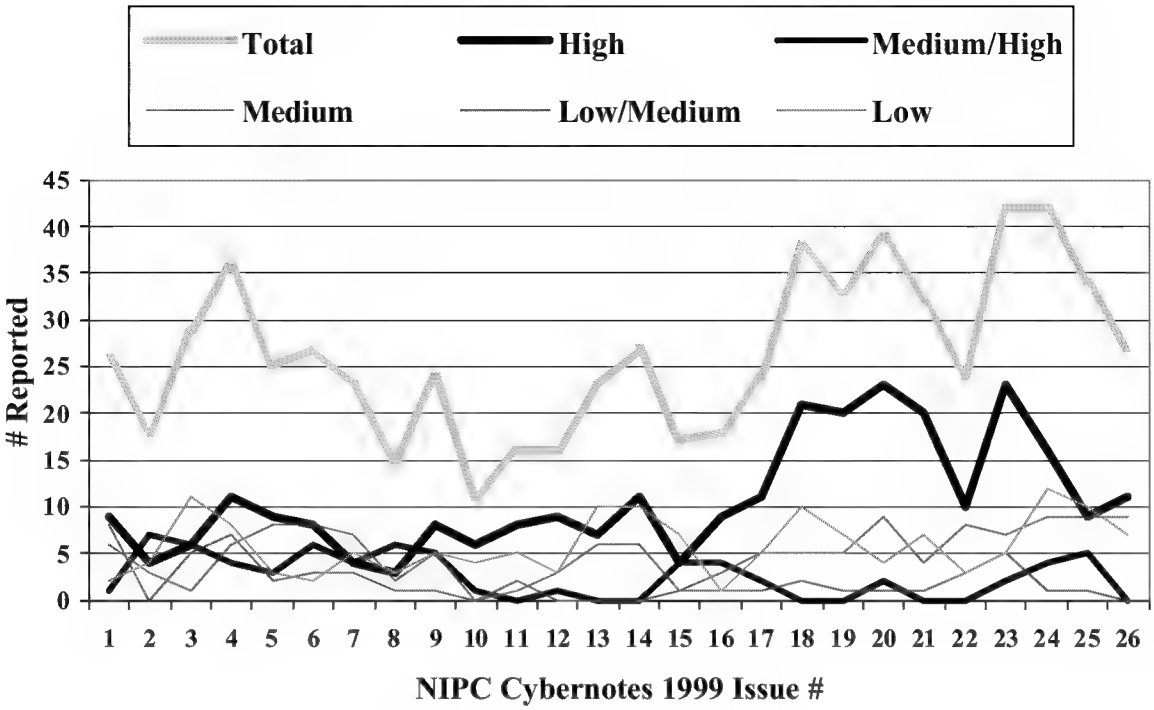
The following chart illustrates the rise in the number of vulnerabilities reported by the CERT/CC at Carnegie Mellon University.

Vulnerabilities Reported by CERT/CC



The NIPC also publishes a bi-weekly report on the number of new vulnerabilities. The following figure illustrates the rise in the number of vulnerabilities, especially those that are considered high risk.

Vulnerabilities Reported by the NIPC



In summary, hacker tools are becoming more powerful and easier to use. At the same time, prevention is much more difficult because the technology changes rapidly. In addition, protection now requires the infected clients, and not just the end victims, to take action. Simply stated, the Internet is a very attractive target for attackers. Internet attacks are easy to do, difficult to detect, hard to trace, and the risk of getting caught is low.

5.3.1. Sample Threats and Vulnerabilities

Some sample threats and vulnerabilities are listed below to illustrate the problem. This is by no means either a comprehensive list of vulnerabilities or a consolidated assessment of the vulnerability of government systems.

(1) **Viruses**. In the past viruses were designed to create a minor annoyance. Viruses have become more malicious and specifically designed for destruction and damage. They are very complex, come in a multitude of forms, and some are "polymorphic". The distinction between viruses, "worms", and trojan horses is narrowing as they converge. In addition to being more malicious, viruses are now easily spread by Email and can spread quickly throughout the Internet. It is even possible under some mailer configurations that a user might automatically open a malicious file received in the form of an email attachment. A good example is the Explore.Zip program, which is a trojan horse (see below). It initially requires a victim to open or run an email attachment in order for the program to install itself and enable further propagation. Once installed, the program behaves as a "worm": it can

propagate itself, without any human interaction, to other networked machines. The Explore.Zip trojan horse has been sent in email messages containing an attached file named *zipped_files.exe*. Some email programs may display this attachment with a "WinZip" icon. Opening the *zipped_files.exe* file causes the program to execute.

(2) **Trojan Horses**. A trojan horse is an apparently useful program that contains hidden functions that exploit the privileges of the user program. A trojan horse does things that the program user did not intend. Intruders rely on users to install the trojan horse that can subsequently subvert the system. Trojan horses can do anything that the user executing the trojan has the privileges to do. This includes deleting files, transmitting files to the intruder, changing files, installing other programs that provide unauthorized network access, gaining root privileges, installing viruses, or installing other trojan horses. Common trojans include Back Orifice, Netbus, Trojan TCP wrappers, and false software upgrades. One of the reasons trojans are a problem is because few software developers and distributors provide a strong means of authentication for software products and, until strong authentication of software is widely available, propagation of malicious software will persist.

(3) **Unexpected Interactions**. Vulnerabilities arise when complex interconnected systems interact in unexpected ways. A good example is the "Cross-site scripting" vulnerability. CERT/CC issued an advisory regarding the possibility for attackers to inject scripts into a web site. This script would then be passed on to unsuspecting users visiting that site and could subsequently be exploited in several ways. For example, an attacker can construct an HTML link to a dynamically generated page on a "trusted site". The link itself could contain a script statement. When an unsuspecting user clicks the link, the trusted site would generate a page containing the script and send it to the victim who, presumably, would allow it to execute since it came from the "trusted site". The impact can be significant. The attacker may gain unauthorized access to an intranet server, have full access to the data retrieved, read fields in forms and send this data to the attacker, gain access to SSL-encrypted connections, and modify the behaviour of forms, including how results are submitted. Note that although certain caution is typically taken when users are visiting web sites, the ability to construct such a link and send it in an e-mail makes this vulnerability extremely dangerous. An attacker can construct the link and put it in an HTML formatted e-mail. If the victim clicks the link from the e-mail the "trusted" site will send the script back to the victim. Worse yet, the attacks may be persistent using "poisoned" cookies that contains the malicious script.

(4) **Denial of Service**. All systems connected to the Internet can be affected by denial-of-service attacks. A denial of service attack is designed to bring a network down by flooding it with large amounts of traffic or by sending malformed packets that cause a computer to crash. Recently they been extensively publicized due to several attacks that brought down major Internet

sites; however, denial of service attacks such as "smurfing", the "ping of death" and "syn flood" have been known for a long time. Powerful new tools to launch distributed denial of service attacks have been released including "Stacheldraht" (German for "barbed wire"), trin00, Tribe FloodNet (TFN), and Tribe FloodNet 2K (TFN2K). Attackers install these tools on hundreds of compromised machines and direct the compromised machines to simultaneous initiate an attack against a single victim. The tools include many features to make traffic difficult to recognize and filter, to execute commands remotely, to spoof the source address (to either hide the true source of the traffic or to make it appear to come from neighbouring machines), to transport traffic over multiple protocols, and to send "decoy" packets to confuse attempts to locate other nodes in the attack network. TFN2K includes attacks designed to crash systems by sending malformed or invalid packets and Stacheldraht uses encrypted communications to cloak its intentions from administrators who might be monitoring the network. Some limited defences do exist, including applications to detect the malicious tools and so-called "egress filtering" to block offending traffic. However, nothing can stop an attacker from launching an attack whenever he so chooses.

(5) **Automatic Execution of Code**. With the aim of making systems user friendly, software vendors have a dangerous practice of turning software products into a programming language and allowing automatic execution of code of unknown origin. This opens the door to malicious code in the form of macros, Java, scripts, and other downloaded executables.

(6) **Software Bugs**. Software complexity and the market pressures for "function rich" user-friendly software results in numerous software bugs that introduce significant vulnerabilities. Operating systems continue to become larger and more complex. Some common vulnerabilities continue to reappear. For example buffer overflow vulnerabilities, which allows remote users to execute arbitrary code with root privileges, exist in numerous programs. Tools to exploit such vulnerabilities continue to be released.

(7) **Poorly Configured Software**. In addition to the problem of updating software with current patches and releases, it is also common for system administrators to introduce vulnerabilities through poorly configured software. This arises because the software may be difficult to configure, the administrators are either inadequately trained or are not familiar with security issues, or users demand services that are insecure.

(8) **Errors or Omissions**. Users introduce significant vulnerabilities through poor practises such as so-called "promiscuous" browsing and execution of software from untrusted sources. Games and greeting cards are potential sources of malicious code. For example, after the elf-bowl game was quickly promulgated to almost all users in many organizations, a false alarm was sounded that claimed that the game included malicious code. Fortunately the alarm was a hoax

(9) **Privacy**. Vulnerabilities that jeopardize privacy have emerged as a major concern on the Internet. Vulnerabilities give rise to privacy issues such as identity theft, tracking users, and access to personal information. Some fault the Internet for a rapid increase in the number of cases of identity theft. In a typical case of identify theft, someone steals an offer for a pre-approved credit card, and submits the application with a change of address. In addition, users actions on the network can be tracked and user profile can be developed using information stored in "cookies". "Cookies" hold personal information that that can be retrieved by any web server one visits. As such, they are an electronic footprint that can be used as a "high tech tracker" to track exactly what users are doing and seeing on a website. Some cookies are useful because they allow users to surf faster and create user profiles to tailor services to meet specific user needs (e.g. what kind of books or CDs one likes). However, this information could also potentially be sold, leaving users an open target for cyber junk mail.

(10) **Authentication**. Authentication is a fundamental requirement for security since it is the basis for almost all security services including access control, privileges, and authorizations. For this reason, authentication vulnerabilities are commonly exploited. The vulnerabilities of passwords and PINs have been known for a long time, yet they continue to be widely used in lieu of stronger authentication techniques. Passwords can be captured and replayed, guessed or broken via password cracking tools, and password files can be captured from insecure computers.

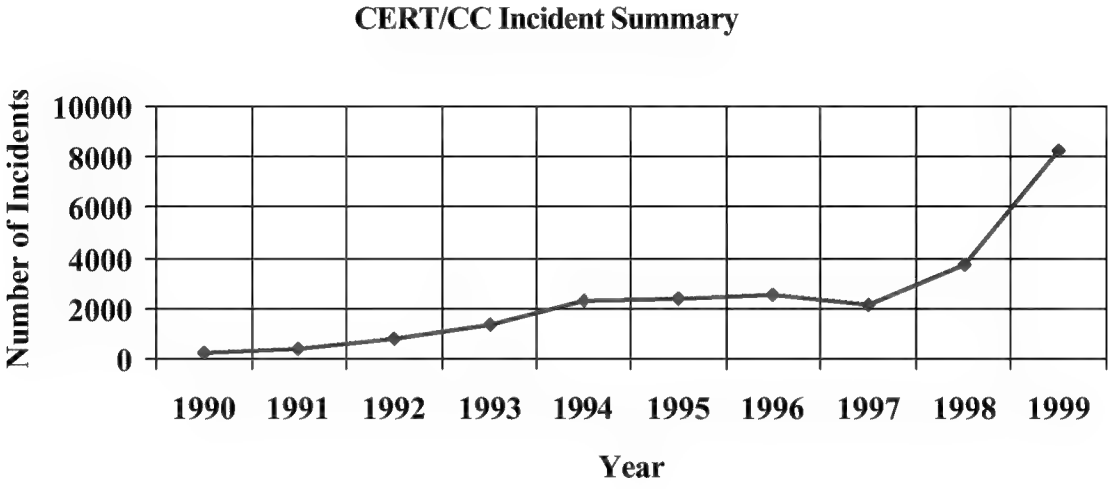
5.4. Internet Security Incidents

The previous section described some of the threats and vulnerabilities associated with the Internet. This section provides some examples of real world Internet security incidents. Most of the incidents reported in this section were reported in the US and other countries. Specific data on Canadian incidents are described later in this report.

The media is filled with examples of information security incidents such as hacking web sites, credit card fraud, damaging viruses such as Melissa and the Explore.Zip Worm, and denial of service attacks. Numerous sources of incident statistics confirm this alarming trend.

In its 2000 Computer Crime and Security Survey[4], the Computer Security Institute again confirmed the continuing trend of increasing security breaches and cyber crime. CSI reports that such breaches are widespread and diverse. The survey reported that financial losses from 273 businesses who responded exceeds $265 million, up from $123 million in 1999. Computer Economics has determined that the economic impact of virus attacks on information systems around the world amounted to $12.1 billion in 1999. Internet-based fraud is the fastest growing criminal activity according to the latest crime figures. Although Internet purchasing makes up only 2% of credit card transactions, the banking industry's credit card research group has shown that the net generates approximately 50% of all credit card complaints. The FBI case load for computer hacking and intrusions has

doubled in each of the last 2 years. The US DoD reports 80-100 incidents per day. The ICSA compiles a list of reported attacks and publishes an annual review [5]. The ICSA 1999 Infosecurity Year-in-Review by Dr. M.E. Kabay provides a detailed list of security incidents in 1999. ICSA believes that hacking incidents are tripling or quadrupling every year, and the risk of viruses is doubling. The CERT/CC at Carnegie Mellon University, which has tracked hacking for 11 years, logged more than 8,000 incidents last year. The following incident summary from CERT/CC illustrates this trend.



5.4.1. Examples of Internet Security Incidents

The following examples illustrate the types of security incidents that have been reported. These examples do not reflect the total scope of Internet security incidents.

(1) **Credit Card Fraud**. In a highly publicized incident, an extortionist hacked into an e-commerce web site and stole 300,000 credit card numbers. The intruder later used the card numbers in an attempt to blackmail the retailer into paying $100,000 in exchange for destroying the sensitive files. When the company refused to comply, the intruder released thousands of the credit card numbers onto the Internet in what turned out to be a public relations disaster for the company. Credit card companies responded by cancelling and replacing the stolen card numbers and notifying affected cardholders by email. Following this attack, MSNBC demonstrated how insecure many similar sites are. MSNBC was given 20 small e-commerce Web sites and simple instructions on how to break in. A reporter at MSNBC said the network was able to break into seven sites within minutes. On these sites, MSNBC found everything from credit card numbers and billing addresses to employee Social Security numbers.

(2) **SATAN Scan**. One of the first vulnerability scanning tools was released on the Internet in 1995 when Dan Farmer conducted a non-intrusive security

survey of approximately 1700 hosts on the Internet and another 500 as a control study. Although this survey is five years old, one could speculate that the situation has only gotten worse because the tools are much more sophisticated. The survey was conducted using a tool called SATAN (Security Administrator's Tool for Analyzing Networks) written by Dan Farmer and Wietse Venema. SATAN is a basic auditing tool that can scan any network connected to the Internet, report vulnerabilities, and suggest fixes for those vulnerabilities. SATAN is freely available on the Internet. Dan Farmer discovered that over sixty percent of the surveyed hosts could be broken into or destroyed, and an additional 9-24% of these same hosts could be broken into by exploiting newly announced bugs (the survey was only checking for known vulnerabilities). When compared to the 500 hosts selected at random as a baseline group, the surveyed hosts were significantly more vulnerable. Since the surveyed sites were considered to be "secure", Farmer concluded that the additional security measures employed by these hosts were ineffective. Furthermore, only three of those sites contacted him to inquire about the unauthorized survey. In addition, Farmer argued that, since SATAN is a very basic tool looking for known vulnerabilities, an additional 10-20% of the hosts could be compromised using more advanced and intrusive break-in techniques. If this is correct, Farmer estimated that 70 to 80 percent of the surveyed hosts have serious security flaws.

(3) **The Internet Auditing Project[6].** An independent consultant in Israel conducted one of the first exhaustive surveys of Internet security in 1998-1999. Using scanning software called BASS, Liraz Siri probed nearly 36 million Internet hosts worldwide over a period of eight months. He was looking specifically for 18 widely known UNIX security vulnerabilities - holes for which vendors have already released patches and other fixes. Siri claimed that about 450,000 servers were susceptible to attack - among them banks, e-commerce sites, nuclear weapons research centers, and even computer security companies.

(4) An attacker obtained 100,000 credit card numbers from the records of a dozen retailers selling their products through Web sites. He used a packet sniffer to capture the numbers as they traversed the Internet. The credit cards had limits between $2,000 and $25,000, putting the potential cost of theft at $1 billion. This type of intruder activity is one form of "identity theft." The attacker was caught when he tried to sell the card numbers to an apparent organized-crime ring that turned out to be the FBI.

(5) Intruders gained unauthorized access to proprietary information on the computer network of a major U.S. corporation. The company was not able to identify the techniques used by the intruders to break through the firewall. The company shut down its Internet connection for 72 hours as a precaution, denying access to legitimate users and cutting customers off from information that the company normally makes available through the Internet. Hundreds and perhaps thousands of credit card numbers, home addresses, and phone

numbers were exposed for months through a security hole on many small Internet auction sites. Records at several sites using older versions of the same auction software were exposed when administrators either did not secure their sites with keys or otherwise failed to use the software properly. The risk varied from site to site, ranging from data immediately accessible with a few mouse clicks to information obtainable through rudimentary hacking. The sites known to have used the software belong to small and medium-sized businesses, in some cases stores trying to capitalize on the e-commerce boom by running their own online auctions. Credit card numbers were not the only information available. One site, for example, also exposed the names, addresses, phone numbers, email, and passwords of more than 100 customers. The same type of information was available, although not as readily, on other sites as well.

(6) In the most serious systematic breach of security ever for British companies, a group of intruders based in the UK broke into the computer systems of at least 12 multinational companies and stole confidential files. The group issued ransom demands of up to £10 million in exchange for the return of the files. Scotland Yard and the FBI are investigating the break-ins, and are scrutinizing email traffic between England and Scotland. They believe the group is highly professional and may be working for information brokers specializing in corporate espionage.

(7) A major credit card company confirmed having received a sizeable ransom demand after intruders stole computer source code and threatened to crash the entire system. The company contacted authorities and began reinforcing its system. It is estimated that if the company's system crashed for just one day, it would cost the company tens of millions in British pounds. Officials are not yet ready to confirm that the attack on the company was the work of the same group responsible for break-ins at other multinational companies in the UK.

(8) **Denial of Service Attacks**. In highly publicized security incidents in February 2000, several major Internet sites including Yahoo, eBay, Amazon.com, CNN, and Buy.com were victims of unprecedented denial of service attacks. These attacks resulted in an enormous public reaction due to the scope of the attacks, the financial losses, and the impact on the confidence of consumers already concerned about disclosing credit card numbers and other personal information online. These attacks also raised the concern about embarrassment and the potential liability of those organizations whose sites were were used to launch the attacks. Using tools described earlier, the intruders commandeered hundreds of separate clients to launch a flood of traffic from different sources to bring the networks down. The attacks followed widespread alerts from CERT/CC. The attacks also lead to a widespread FBI investigation and renewed emphasis on computer security. The President held a meeting with senior security experts from the private sector. The ICSA formed a private sector alliance of Internet service providers (ISPs), industry professionals and corporations committed to the widespread

adoption of security measures to address Distributed Denial of Service Attacks. This alliance is called the Alliance for Internet Security.

(9) **Solar Sunrise, Moonlight Maze, and Operation Eligible Receiver**. These were high profile events within the US government over the past two years. The Solar Sunrise attack into DoD computer networks used a well-known vulnerability in the operating system. Moonlight Maze tracked a series of widespread "distributed coordinated attacks" on the US Department of Defense, other federal government agencies and private sector computer networks. In Operation Eligible Receiver, the US Government demonstrated that they could launch successful attacks to obtain "root access", the highest level of control, on many government networks. The Canadian Department of National Defence conducted similar exercises on DND networks.

6. THE THREAT TO CANADIAN NETWORKS

One of the difficulties in assessing the threat to Canadian networks and systems is that there is little Canadian threat data available. Most of the available data on Internet-based threats is generic in nature or is based on experience in the United States. Fortunately, most of the highly publicized security incidents have not taken place in Canada.

There have, however, been several reports that Internet attacks have either originated from, or passed through, sites in Canada. The Ottawa Citizen published an article claiming that the US Defense Intelligence Agency estimates that 80% of the attacks on US systems originate from or pass through Canada. Although this estimate could be questioned, the fact remains that Canada and the United States share many common information infrastructures and therefore share many of the same risks.

Accurate data regarding security threats in Canada are not available because few organizations monitor their networks closely, few incidents are reported publicly, and a coordinated reporting structure to share information does not yet exist. Information regarding the threats and vulnerabilities of Canadian networks is therefore only available in a piece meal fashion. Unfortunately, these facts may make Canadians more complacent about the risks than they should be.

For the purpose of this report, a limited amount of information was obtained to provide a ***snapshot of the risks*** to Canadian information systems. This information was provided by a number of available sources including monitoring of selected federal government Internet sites, RCMP, CanCERT, members of the PSCIOC Subcommittee on Information Protection, and the results from Operation Caveat conducted during the Y2K transition period. Some limited reporting from federal, provincial and municipal organizations is continuing and a standardized reporting format has recently been adopted.

6.1. Threats to Selected Government of Canada Internet Sites

This section includes extracts from the report "Threats to Selected Government of Canada Internet Sites"[7] released by the Communications Security Establishment in November 1999.

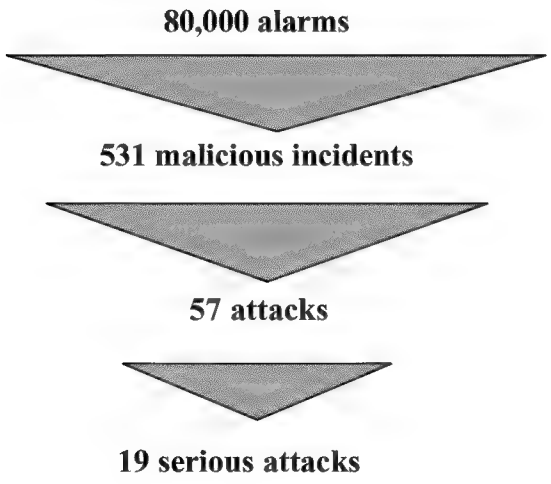
6.1.1. Aim

The Government of Canada conducted a project to collect real-world data to objectively assess the current level of threat activity against GoC Internet points of presence. To support the gathering of threat data, a network intrusion detection system (IDS) was used to capture threat activity at the Internet point of presence for six federal departments. A network IDS is the equivalent of an alarm system for a network – it monitors network traffic and when malicious activity is observed, it raises an alarm. Network IDS sensors were installed at each of the participating department Internet points of presence, typically in front of their Internet firewall, and operated for a period of two months. During this period, alarms from these sensors were collected, centrally logged and then analyzed to identify threat activity.

During the observation period, the six IDS sensors generated more than 80,000 alarms. As normal (non-malicious) network traffic can trigger IDS sensor alarms, these 'raw' alarms were analyzed to identify those which represented true threat activity. Based on this analysis, a total of 531 incidents of malicious activity were identified (a single incident could involve multiple IDS alarms). The vast majority (474 or 89%) of the threat activity was associated with the initial information gathering phase of an attack – essentially attackers mapping out and conducting reconnaissance to identify vulnerabilities of potential targets. Actual attempts to conduct denial of service attacks (crash systems or clog networks), or gain unauthorized access to systems or networks represent the remaining 11% of the total. This included 34 denial of service attacks and 23 attempts to gain unauthorized access. Where there was a possibility that an attack may have been successful or could have potentially serious impact, the department was notified for follow-up action. A total of 19 incidents were considered serious enough (e.g., an attempt to retrieve the system password file) to warrant further investigation by departments.

The following graphic illustrates the analysis process. It is emphasized that this analysis is a very resource intensive and time consuming process.

Analysis of IDS Alarms



The following chart summarizes the results of the threat analysis:

Incident Summary for Selected Federal Internet Sites July-August 1999

Incident Class	Total Incidents	Percentage of Total
Scanning	474	89%
Access Attempts	23	5%
Denial of Service	34	6%
Totals	531	100%

There were several limitations regarding this study. While the data is valid for demonstrating the existence of network threats against federal Internet points of presence, it only provides a small window into the actual level of threat activity. In addition, any observed trends or patterns do not necessarily extend beyond the activities that were successfully observed. Further, it should be noted that only six of the more than 125 federal Internet points of presence were included in this project, and the IDS sensors were only operational for slightly more than two months. The threat activity certainly did not cease at the end of the project, and it most certainly is not limited to just the six departments participating in the project.

6.1.2. Observations

(1) There is a Threat to the Government of Canada. The report concludes that federal Internet points of presence are being probed, scanned and attacked on a regular basis. While the level of threat activity varied across the six federal sites participating in this project, a typical federal Internet point of presence is subject to ***10 or more threat incidents per week***. In some cases, peaks of greater than 40 incidents were observed for a site during a week.

Of note, most of the denial of service and unauthorized access activity against federal systems and networks is illegal under Canadian law.

(2) The Threat Appears to be Global. While 81% of the threat activity appeared to originate from Canada, the UK or the US, activity from a total of 33 different countries was observed. While the observed malicious network traffic originated from a computer system in the identified country, the actual attacker may not have been from that country. More sophisticated hackers often conduct attacks from other 'hacked' systems in an effort to hide their true identity and complicate law enforcement efforts, and have been know to route their attacks through multiple systems located around the world. As a result, care must be taken in affixing the country of origin to attacks – the apparent source computer may not be the true origin of the attacker.

(3) Automated Attacks Tools Are Being Used. A significant portion of the threat activity is being conducted using automated tools that search large blocks of IP address space for targets with a particular vulnerability that can be exploited. These automated tools systematically scan for possible targets, and the attackers are not normally concerned about who "owns" the system. As such, it should be assumed that any system accessible from the Internet will be subject to attack (i.e., "security by obscurity" does not work). This further suggests that a portion of the observed threat activity probably originated from what is commonly referred to as "script kiddies" using pre-scripted attacks. Despite being unfamiliar with the details of how to attack and exploit a system, these novice users can perpetrate attacks against systems and networks given the user-friendly ("point and shoot") nature of some of the available attack tools.

(3) IDS Detection Criteria Impacted Results. The IDS detection criteria selected for this project was designed to minimize the inadvertent capture of user data. As such, 44 of the 160 IDS intrusion signatures were disabled. In all probability, had these signatures been enabled, a higher level of activity would have been observed, particularly for unauthorized access attempts against e-mail, FTP, Web and network news servers.

(4) Network IDS Provides Insight into Network Threat Activity. As demonstrated by this project, network IDS can provide insight into the threat activity against a network. However, it must be kept in mind that network intrusion detection is a relatively new, but maturing, technology. While the capabilities of network IDS technology continue to improve, none are 100% effective at detecting attacks. As a result, network IDSs are most effective when supplemented by network traffic capture, firewall and host-based logging, and host-based intrusion detection. By combining and analyzing information from all of these sources, a more accurate and complete view of the threat activity against a network is possible. This analysis, however, is still very labour intensive.

It was not a goal of this project to measure the effectiveness of the network intrusion detection system in detecting attacks. However, it has been proven through this project that the detection of at least a specific subset of attacks is possible. To more fully understand network IDS capabilities a wide range of attack testing to categorize the effectiveness of network IDS systems would be required.

(5) Layered Network Defences. Network IDSs are not a "silver bullet" that will solve all network security problems – they are only ***one part of an effective IT security architecture***. They complement the protection capabilities of firewalls by providing a network "alarm" system for potentially malicious traffic. IDSs also have some limitations as to the types of attacks they can effectively identify. Ideally, network IDS should be supplemented by host-based intrusion detection and logging to provide a more complete picture of the current state of the network.

It is also important to make sure that the implemented security architecture provides sufficient coverage for the threat of concern. Alarming the Internet "front door" with a network IDS does not solve the problem if the attacker is coming through a back door (e.g. by connecting directly to the network via a modem) or if the attacker is already in

the building (e.g. internal threat). Clearly the threat must be considered in selecting and placing intrusion detection systems.

(6) Threat Activity Varies With Time. In terms of distribution as a function of time, attacks are most frequent during regular business hours, followed by evenings. Threat activities occur about twice as often on weekdays versus weekends. The nature of the threat activity also varies with time. The most likely cause of this is the identification of new vulnerabilities or the release of a new or updated attack tool. For example, at the beginning of the assessment there was a lot of threat activity searching for vulnerable web server scripts, but this decreased as the project progressed. Similarly, towards the end of the assessment period a number of UDP bomb attacks were observed, an attack type that had not been seen before.

In order to get a clearer picture of factors that influence activity against federal systems, threat activity would have to be assessed for a longer period (to span seasons), while keeping track of the release of new tools, discovery of new vulnerabilities or exploits, etc.

6.1.3. Recommendations

(1) Intrusion Detection and Response. Network IDSs are an important component of an overall network security architecture. They provide network administrators with insight into activity on their networks, and provide them with an "alarm" system that identifies potentially malicious network traffic.

Intrusion detection involves much more than simply implementing the technology. Analyzing alarms is a resource intensive effort that must be supported by sound policy and sufficient resources. Inevitably, when an intrusion detection system is deployed, intrusion attempts will be found. Having discovered an intrusion attempt, there is a responsibility to respond by either confirming if it was successful, securing the target network or systems, investigating the threat, or possibly all three. In order to accomplish this effectively, policies and guidance are required regarding the goals of intrusion detection, configuration of the devices, and how to respond to attacks. As was evidenced in this project, there is no clear picture of the action that should be taken upon discovering that an attempted intrusion has occurred. Guidelines for incident response were not available, and often the participating departments were often not adequately prepared to take appropriate action when a potentially serious incident was reported.

(2) Intrusion Detection Strategy. The report recommended development of a well-defined strategy for implementing network intrusion detection within the overall security architecture. The results of this project are simply a snapshot of a portion of the threat environment at a particular point of time. It would be beneficial to implement intrusion detection for the collection of threat data on an ongoing basis, if not at every location, then at least at strategic points within the overall network infrastructure. A government-wide intrusion detection framework could provide a viable baseline of data for assessing the threat against the network infrastructure.

(3) Reporting and Response Capability. Once the collection of intrusion detection data begins, questions quickly arise as to how to respond to detected threat activity, and where to report it. If incident reporting and response were coordinated and standardized, the sharing of information and protection against threats would be simplified. Specification of a common information format would make trend and pattern analysis a feasible activity and the output threat data could be used by all participants to further improve their security posture. It would also be possible to identify wide scale attacks involving multiple departments. Establishing central contact would simplify responses to an incident involving external entities. Establishing an incident reporting and response capability is highly recommended.

6.2. RCMP Computer Crime Statistics

The following table illustrates the increasing number of computer-related cases handled by the RCMP across the country. The categories reflect the illegal computer-related activities defined in the Criminal Code.

RCMP Computer Related Investigations

Offence Type	1998	1999	First Quarter 2000
Mischief to data	111	192	46
Unauthorized use of computer	130	158	62
Pornography	19	9	3
Copyright act violations	110	173	35
Total	**370**	**532**	**146**

6.3. CanCERT

CanCERT regularly receives incident reports from sources within Canada as well as reports from international sources regarding incidents originating from Canada.

CanCERT™ is a trusted centre for the collection and dissemination of information related to networked computer threats, vulnerabilities, incidents and incident responses for Canadian government, business and academic organizations. CanCERT™ was founded in 1977 and is currently operated solely by the private firm Electronic Warfare Associates-Canada Ltd. (EWA-Canada). CanCERT™ maintains affiliations with global Incident Response Teams via the Forum of Incident Response and Security teams (FIRST). FIRST is an international consortium of computer incident response and security teams who work together to handle computer security incidents and to promote preventive activities.

The following table summarizes the incidents detected by CanCERT on its own infrastructure. Note that CanCERT does not have incident data available from broader sources because a centralized reporting structure does not exist in Canada.

CanCERT Incident Summary 1999

Incident Class	Total Incidents	Percentage of Total
Scanning	174	66%
Access Attempts	52	20%
Denial of Service	36	14%
Totals	262	100%

6.4. Provincial Information

In a large part due to the efforts of the Subcommittee on Information Protection, many of the provinces have, or are in the process of establishing, a capability to detect and react to Internet security threats. Threat information has been reported to the Subcommittee on Information Protection and to the incident response team established during Operation Caveat described below. This section provides a brief snapshot of threat information reported by various provinces.

The provinces have also been active in the area of security awareness and education. In particular, Saskatchewan conducted an intensive two-day awareness session[8] that was well attended. The content of this session was provided to all members of the Subcommittee on Information Protection.

6.4.1. Web Sites Hacked

These incidents were reported in all jurisdictions including the federal government (e.g. DND and HRDC), provinces (Newfoundland), and municipalities (Mississauga). Although these incidents may be seen by some as a mere nuisance, they can have a significant impact on public trust and confidence. Such attacks indicate that many web sites are vulnerable and may also give the impression that sensitive systems are equally vulnerable. Worse yet, information on web sites may be altered causing damage to those who rely on it. What is important is that solutions do exist. Newfoundland, for example, has implemented a proxy server solution to secure the Government of Newfoundland web site.

6.4.2. Viruses

Again, virus incidents were widely reported in all jurisdictions. For example, the email system in one federal department was shut down for several days due to the Explore.Zip trojan. The most significant virus impact was due to the Melissa virus. The Government of British Columbia estimated the cost impact of the Melissa virus to be in the order of

$250,000, and as a consequence implemented an effective Virus Incident Response Team (VIRT). As a result of the VIRT, the number of virus incidents has been dramatically reduced and consolidation of resources reduced the cost of virus defence. British Columbia is a leader with regards to virus detection and response.

6.4.3. Information Protection Centers

Most provinces have implemented or are in the process of implementing Information Protection Centers (IPCs), including Intrusion Detection Systems, to detect and respond to malicious activity. The Government of Manitoba is a leader in this area and provided incident data to the Subcommittee on Information Protection on a regular basis.

6.4.4. Trojan Horses

Implementation of Information Protection Centers in the provinces has started to provide more insight into the nature of the threats. For example, during an IPC pilot one province detected that the trojan horse "Back Orifice" was installed on an internal computer and was subsequently sending sensitive information to an external computer in the United States. This example highlights the need to monitor *outgoing* network activity as well as *incoming*.

6.5. Operation Caveat

As Y2K approached there was an increasing concern about hacker activity. Hacker groups issued invitations to a "hackfest", new distributed denial of service attack tools appeared, and Y2K viruses were discovered. In response, CSE established and operated Project Caveat for a short time period over the Y2K transition period[9]. On a broader scale, CSE joined forces with CanCERT, nine federal departments, and all ten provinces to share information on reported activity and to coordinate the response. These coordinated reports were also provided to the Y2K Intelligence Response Team.

The information was shared during daily conference calls that were extremely effective in rapidly reporting malicious activity, to provide alerts on current threats and vulnerabilities, and to coordinate detection and analysis of wide spread malicious activity. Participants were also able to seek and give guidance regarding detection and analysis of incidents. The conference calls were so effective that they were extended after the Y2K period, albeit less frequently.

Fortunately, it turned out that the anticipated increase in hacker activity did not happen during the Y2K period. Despite this, several malicious events were detected and the experience highlighted the following significant findings.

6.5.1. Reporting Sources to Internet Service Providers

There were frequent reports of malicious activity originating from certain Internet Service Providers. In a coordinated response, CanCERT reported such activity either to an International Forum or to the ISP concerned. As a result of these referrals and

interaction with the ISPs, the Internet accounts of the originators of the malicious activity were revoked.

6.5.2. The Threat to Interconnected Systems

Analysis of an attack originating from a provincial agency revealed that the system had been hacked and was subsequently used to launch further attacks. Not only did the coordinated approach serve to detect that the provincial agency had been hacked, it also provided insight into the nature of the threat in a widely interconnected environment. Government computer systems are vulnerable to security gaps in other interconnected systems. This will be an increasing concern as more and more government programs are on-line because large numbers of external connections will exist to provide citizens and businesses access to government applications.

6.5.3. Detection and Analysis of Wide Spread Threats

The coordinated approach also detected a wide scale network mapping activity across Canada that would not have otherwise been detected. Early in the analysis process, CanCERT issued a draft alert noting that they had received and reviewed log data from a variety of sources, and believed that a wide-scale, distributed, and possibly coordinated scan of the Canadian Internet address space was underway. This scan appeared to be mapping the Canadian Internet address space looking for hosts that are 'alive', potentially to identify possible targets for later compromise. The scan was designed to be stealthy and to bypass screening routers and firewalls. The immediate impact was minimal as the traffic levels generated by the scan are extremely low. However, the information gained from the scan could be used to target systems for later exploit.

This activity used a technique called a "slow scan" in which probes occur in very short intervals over a long period of time. Such attacks are extremely difficult to detect and would have gone unnoticed in most jurisdictions had they not been alerted by the coordination center. The coordinated response not only alerted all participants of the threat, it facilitated central analysis of a potentially malicious event that occurred across the country. Although this event was not a major threat, it did highlight the need for a coordinated response to counter more sophisticated distributed and coordinated attack techniques.

7. BUILDING A TRUSTED INFORMATION ENVIRONMENT

Public Sector CIOs should ensure that governments employ adequate management controls, policies, and technical measures ***to provide a trusted information environment suitable for e-government.*** Information should be protected from unauthorized access and unintended modification, destruction, disclosure, or other endangerment. There are no easy solutions. Although security is troubling, ***a well-managed security program can significantly reduce the risks***.

This is not a simple task. The level of understanding of security threats, exposures, safeguards, practices, and priorities varies widely. There is neither a single standard architecture nor any "one-size-fits all" security solution. Executives should regard information security as a contributor to governments' well being, rather than a cost center or an insurance policy. As a result, assessing risks, setting priorities, and committing the necessary resources presents a considerable challenge. This task involves much more than technology, it requires fundamental management practices.

Risk avoidance is impossible. There are compelling reasons to meet the government on-line objectives, and the challenge is to find the right balance between business and security imperatives. The risk-avoidance approach to information security fails to take into account government operational imperatives, and does not provide solutions that are practical and proportional to the risks they are designed to address. Risk avoidance also disproportionately consumes financial resources relative to the degree of risk it reduces. At the same time, security measures are available to prevent persistent and continued breaches of security, but they are typically not implemented due to concerns of cost or performance. To be effective, a security program must focus on providing value-added support to business processes, government operations, and decision-makers. Without this focus, security will either be a roadblock or it will be ignored.

7.1. Privacy and Security Requirements for Electronic Security Delivery

Because the Internet is the vehicle of choice for electronic service delivery solutions, privacy and security are crucial issues. It is essential that citizens trust government to protect their information. Most transactions between government and citizens involve personal, sensitive, proprietary, or financial information. Surveys on Canadians' attitudes about electronic commerce and other electronic services repeatedly reveal concerns about the security and privacy of transmitted information. Canadians will only accept and use secure electronic service delivery initiatives if they have faith in government's commitment to protect their private information. Any secure electronic service delivery solution must respond to this fundamental concern.

Citizens demand more of government – especially when information security is the issue. When a citizen obtains government services using electronic delivery, they are acting on the expectation that the government ***has already applied*** an appropriate standard of care with respect to the protection of their personal information. Financial and other constraints may occasionally force government officials to adopt less than "perfect"

solutions; however, surveys consistently indicate that citizens hold government accountable to higher standards when it comes to information security. Accordingly, they expect that government security practices and procedures will provide the degree of security required. Doing so will ensure Canadians' trust and confidence in government's secure electronic service delivery solutions.

CIOs operate in an imperfect world of financial constraints, time pressures and political priorities. In the realm of security, governments must exercise an appropriate standard of care by adhering to emerging protection standards. To do this - to ensure the trust and confidence of Canadians - there must be a commitment to move from "less perfect" to "more perfect" secure electronic service delivery solutions.

The use of electronic government services by citizens on a large scale necessitates a shift in the strategic focus of governments. From a "government" perspective, security mechanisms are designed to protect the government from loss or damage. From a "citizen" perspective, security mechanisms must be designed to safeguard the privacy of the citizen's information. Traditional threat-risk assessments do not distinguish between security and privacy safeguards. What the government considers security, Canadians view as privacy protection.

One unintended result of offering citizens electronic service delivery is the unprecedented level of connectivity they will have to internal government systems. This proximity will make it necessary for government to implement measures to prevent inadvertent exposures of these systems to unauthorized access.

7.2. Security Management

Security management involves ***managing risks*** and practising ***an appropriate standard of care.*** Management is responsible for the security of all information and supporting systems, and for addressing the risks imposed by connections to other systems. Management should ensure that information security risks are clearly identified and efficiently managed. Management is also responsible for identifying the resources to be protected and the measures to be used. The information security staff is responsible for articulating policy, for providing expert guidance and direction, for measuring compliance, for noting variances, and for recommending corrective action.

The CIOs cannot do this alone. Business managers, information systems specialists, and security practitioners must collaborate effectively to achieve a balanced solution. In particular, it important that the ***business community be involved in the process*** and that security is seen as a business issue. Involvement of the business community will provide a better understanding of the trade-offs involved to ensure a balanced approach. Security should be viewed as an enabler of change and as a necessary component of a business process.

Governments should ensure that information systems have adequate management control and accountability, balanced with the business needs of the organization. Information protection can be achieved only through effective management and oversight. Some

governments have assigned the oversight of information security to organizations outside of the CIO, some have assigned this to specialized committees, and some have created combined board/management committees to oversee this area. In whatever manner a government proceeds, sound management control and oversight are fundamental requirements.

The Institute of Internal Auditors (IIA) Board-level Guidance Report[10] provides guidance for board members and executive management of organizations with critical information infrastructures. This report was prepared by IIA in partnering with the U.S. Critical Infrastructure Assurance Office (CIAO). The IIA is an international professional association for the promotion and development of the practice of internal auditing. The CIAO requested IIA to provide information on business risks associated with information security and to focus on information security practices.

The United States General Accounting Office (GAO) also stressed the fundamental importance of security management[11]. The GAO report states that while many factors have contributed to weak security in the US federal government, poor security program management is the fundamental cause of poor computer security. A similar situation exists in many government jurisdictions in Canada. To provide greater assurance for critical information systems, the GAO identified seven areas for improvement:

(1) Clearly defined roles and responsibilities

(2) Specific risk-based standards to determine the level of security controls required and the level of rigor with which to enforce them

(3) Routine evaluations of security controls

(4) Adequate executive level oversight

(5) Adequate technical expertise

(6) Adequate funding

(7) Comprehensive incident response and coordination

7.2.1. Key Questions for CIOs

Asking the right questions is important in seeking assurance that a sound information security program is in place. In consultation with management, the IIA identified the following questions from a broad-based set of information security principles. These questions may be useful for CIOs.

(1) What management system have we established to assure effective assignment of accountability for the security of our information and supporting technology resources?

(2) What has management done to assure that all parties know, understand, and accept the importance of adhering to sound information security?

(3) What has management done to assure that we are using our information assets and administering information security in an ethical manner?

(4) What has management done to assure that the perspectives and considerations of all interested and affected parties are considered and balanced in developing our information security policy?

(5) What cost/benefit risk and due care analysis has been applied to the selection of our information security controls?

(6) How have we coordinated and integrated information security with our overall policies and procedures to create and maintain effective security throughout our information systems?

(7) What capabilities do we have to assure that failures involving information technology or its management will not endanger the organization, its supported business units, its neighbours, or their information assets, and will not impair their ability to operate? (Consider requirements for timeliness, availability, and reliability.)

(8) What capabilities do we have to assure that risks associated with information and supporting technology resources are effectively assessed on an appropriate periodic basis, or as otherwise required, and managed accordingly?

(9) How do we assure that our information security measures are fair and legal?

(10) How effectively do we share information about our loss and threat experience with our peer organizations?

7.2.2. Risk Management

Governments need to manage threats to information in the same way as one would manage risk to personal belongings: determine which items warrant protection, consider possible threats to them, and assess how vulnerable they are to a threat. When one knows the extent of the threats, one can accept the risk, reduce it by safeguarding the items, or transfer it (e.g. buy insurance).

Information security risk management involves a similar process. First identify critical operations and associated assets, including the supporting processes and systems, then evaluate the threats to those processes and systems. Of particular concern are those exposures that, if exploited, will result in an unacceptable impact to the organization.

The impact of an attack against the broad range of government information assets and business processes varies widely. Conducting a comprehensive risk assessment of every

aspect of government information systems will provide valuable information, but it will prove too costly and operationally impractical. Risk assessments provide a means for identifying potential problems and evaluating their severity, but those problems often are well-documented from experience and their solutions have already been expressed in policy and security standards.

The risk management process includes three components of risk equation: asset, threat, and vulnerability. The goal is to reduce risk by reducing some component of the risk equation. For example, controls that eliminate a system vulnerability or prevent a threat will reduce the level of risk.

Risk assessment is a process of choosing controls based on probabilities of loss and the impact of the loss. The following questions form the foundation for determining the level of risk associated with potential threats:

(1) Threat Events-What could go wrong?

(2) Frequency-How often could it happen?

(3) Impact-What are the consequences?

(4) Confidence/Uncertainty-How certain are the answers to the first three questions?

Once this is complete, answers to the following questions will help make informed decisions about whether to accept, avoid, or transfer risks:

(1) What can be done about unacceptable risks?

(2) How much will it cost?

(3) Are selected safeguards effective?

(4) What is the residual risk?

Guidelines are widely available to assist with the risk management process. Examples include RCMP's "Guide to Threat and Risk Assessment for Information Technology" and CSE's "A Guide to Security Risk Management for Information Technology Systems" (MG-2).

7.2.3. The Need for Continuous Risk Management

Threat and Risk Assessments based on such guidelines have been in place for a long time. Unfortunately, static risk assessments are no longer sufficient in the dynamic world of the Internet. Technology is changing rapidly, and new systems, network connections and applications are continually being deployed. In addition, new threats, vulnerabilities, and exploit scripts are being identified on a continuous basis. If an organization is not prepared to react quickly when new instances of an exploitable vulnerability are

introduced the risk exposure is significantly increased. This occurs because it usually does not take long between the time a vulnerability is first detected and the time when scripts to exploit the vulnerability are widely available and in use. This phenomenon is well understood in the area of virus protection and anti-virus tools are usually updated on a regular basis to keep pace with new viruses.

The risk management process should include a process ***to continuously monitor the "health" of the network*** and take action when the security risks change. This requires an element of "active" information protection including elements such as:

(1) Continuously monitor what is going on in the network using audit logs and intrusion detection systems;

(2) Perform regular vulnerability assessments and security audits;

(3) Monitor and react to new security alerts, threats and vulnerabilities as they are identified; and

(4) Optionally perform penetration testing.

New risk management processes are being developed to address the dynamic nature of the Internet and the specific requirements of critical information infrastructures. An example of such a process is the Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework (OCTAVE) Framework[12] developed by the Software Engineering Institute at Carnegie Mellon University. Aspect of Continuous Risk Management[13] can also be applied to security.

7.3. Policies and Controls

7.3.1. Legal Framework

One of the goals of information security is to implement and maintain a reasonable standard of care, appropriate in the circumstances, and based on legal, policy and professional standards - as well as public opinion. Meeting the legal standard of care helps manage the risk of liability, both regulatory and in negligence. What is the standard of care required, though, has yet to be defined. It must be "reasonable" in light of the risks, and it must be equal to the standards common in the industry, if they yet exist. Governments may be held to higher standards in order to achieve the trust and confidence of citizens and to ensure that information vital to the well-being of the country is adequately protected.

The protection of information is necessary to enhance the security and privacy of information. Obligations to protect the personal information of citizens are found in, for federal Government institutions, the *Privacy Act* of Canada, and many provincial government institutions are subject to similar legislation at the provincial level. Bill C-6, the proposed *Personal Information Protection and Electronic Documents Act,* will impose similar obligations on federally regulated institutions in the private sector.

However, the very steps that must be taken to achieve the aforementioned goals, and to meet the requisite standards of care, themselves raise serious legal issues that must be considered. Certain monitoring activities, for example, need to be examined in light of privacy legislation, the *Charter of Rights and Freedoms*, the *Criminal Code of Canada*, among others.

7.3.2. Policies

In a broad sense, information security policies are management directives that establish the business goals, security framework, responsibilities, and governance. Establishing a security policy is the first step in improving information security. If a security policy already exists, it should be regularly reviewed within the context of the changing security environment associated with e-government.

There is considerable information available to assist in the development of security policy. As a minimum the policy should:

(1) Emphasize the value and dependence on information, and the importance of information security to the organization;

(2) Identify the goals and principles of effective information security;

(3) Identify minimum security regulations and compliance requirements. This includes elements such as risk management policy, classification and labelling of information, personnel and physical security, legal and contractual requirements, system development and operation, business continuity planning, incident reporting and response requirements, violation enforcement, and security awareness and education;

(4) Define roles, responsibilities, and accountabilities; and

(5) Any critical information system or issue-specific requirements.

7.3.3. Standards and Best Practices

Developing a security infrastructure involves designing and implementing administrative, procedural, and technical controls that mitigate security risks. Implementing ***sound security policies, standards, and best practises will greatly help reduce the overall risk*** exposure while demonstrating an appropriate standard of care.

At the same time, information owners, custodians, and users must know that they are responsible for achieving the stated security objectives. Governments should regularly evaluate security measures in a practical manner.

Standards and best practises are the most direct and efficient means of achieving a standard of due care. However, not all controls apply to, or are practical in, every situation. Some situations warrant development of special or selective controls based on a focused risk assessment. In the end, a government's security posture will be defined

primarily by policies, standards, and best practices, augmented by additional controls as required based on a focused risk assessment.

Security standards and best practices are defined in numerous sources, some of which are listed below. In general, all of these sources advocate security principles similar to those described in this report.

(1) "Guidelines for the Management of IT Security", ISO/IEC TR 13335, 1997 (Part 1- Concepts and Models for IT Security, Part 2 – Management and Planning IT Security, Part 3 – Techniques for the Management of IT Security, Part 4 – Selection of Safeguards)

(2) "Guidelines for the Security of Information" - Organization for Economic Cooperation and Development, Paris: OECD, 1992-last updated 1997

(3) "Generally Accepted System Security Principles – Pervasive Principles", International Information Security Foundation, California: Auerbach Publications – Information Systems Security, 1999.

(4) "British Standard 7799 - A Code of Practice for Information Security Management, and Specification for Information Security Management Systems", By the British Department of Trade and Industry Commercial IT Security Group with the British Standards Institution. London: BSI-DISK, 1993

(5) "Managing Security of Information" an International Information Technology Guideline, By the International Federation of Accountants Information Technology Committee, New York, NY. 1998

(6) "Electronic Commerce - Trends, Technology and the Security, Control and Audit Implications", Prepared for the Institute of Internal Auditors (IIA) by the International Federation of Accountants Information Technology Committee, New York, NY. 1998

(7) "Practices for Securing Critical Information Assets", Critical Infrastructure Assurance Office, January 2000

(8) "Guide for Developing Security Plans for Information Technology Systems", NIST Computer Security Online Special Publications

(9) "Canadian Handbook on Information Technology Security (MG-9)", Communications Security Establishment

(10) "Managing the Security of Information An Executive Guide", International Federation of Accountants (IFAC)

(11) "Information Security Management - Practices of Leading Organizations", US General Accounting Office - Executive Guide

(12) "Information Security Risk Assessment Guide - Practices of Leading Organizations", US General Accounting Office - Exposure Draft

(13) "Software Capability Maturity Model (SW-CMM) and System Engineering Capability Maturity Model (SE-CMM)", Software Engineering Institute (SEI) Carnegie Mellon University

(14) "Information Technology Security Maturity Framework (draft)", US CIO Council Security Subcommittee

(15) "Technical Security Standard for Information Technology", RCMP, 1997

Despite an evolving security environment, the goal of information security fundamentally has not changed. That is, the prudent protection of information assets by the use of policies, standards, and best practices that implement an appropriate standard of due care. This is not any different from how governments deal with other risks.

7.4. Layered Security Architecture

Technical security solutions must align with the overall security strategy. Governments should not rush to implement narrowly targeted security "point solutions": a firewall here, virus protection there. Such quick fixes may do more harm than good because they likely will not provide a complete and consistent level of protection, and may provide a false sense of security. A sound overall security architecture is essential to satisfy the demanding security requirements in an Internet environment.

The goal of the security architecture is to define a set of technical safeguards and standards to provide a consistent and complete security posture. The architecture should define the common security infrastructure, a set of common solutions and standards that can be applied across organizations, and a range of technical safeguards required to support business processes.

A ***security architecture is derived from legal, policy and business imperatives***. From these, core security principles can be defined to guide the evolution of the architecture. Principles could include items such as:

(1) The security architecture should be based on a layered approach that provides a consistent level of protection across the wide range of threats and vulnerabilities;

(2) Absolute risk avoidance is impossible. The security architecture should therefore include an active detection and response capability to react quickly when an incident occurs;

(3) The security architecture should provide a balanced level of protection based on the principles of risk management. The architecture should provide a range of security solutions that take into account the relative risks, sensitivity or importance of the information assets, and the business drivers;

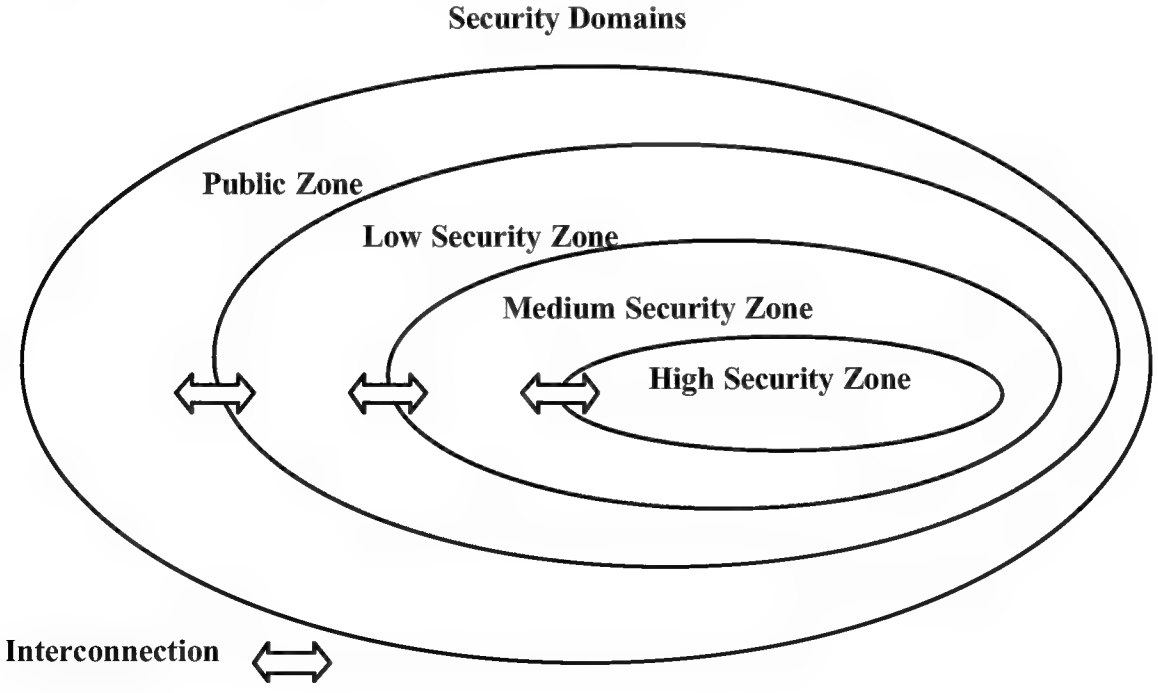
(4) The security architecture should take into account emerging standards in order to provide an appropriate standard of care;

(5) End-to-end security is required for the protection of transactions with sensitive information or financial/legal implications;

(6) The security architecture should protect critical government information infrastructures including those that impact national security, economic security, and crucial health/safety activities.

Implementing a security architecture requires a ***structured process*** that takes into account both security and business requirements. The first step is to define a logical model that identifies a set of security domains with similar security requirements in terms of confidentiality, integrity, and availability. These domains should based on the business processes and information that need to be protected. Once the security requirements and security services for each of these domains have been determined, a set of technology solutions and standards can be defined to satisfy those requirements. These solutions should be determined based on risk management principles. The final step is to conduct a gap analysis between the baseline infrastructure and the target architecture in order to develop an action plan and set implementation priorities.

The following diagram depicts the notion of security domains within a layered security architecture. The circles represent security domains, or zones, with similar security requirements. These domains can be logically separated using security technologies, but can also be interconnected using appropriate security safeguards.

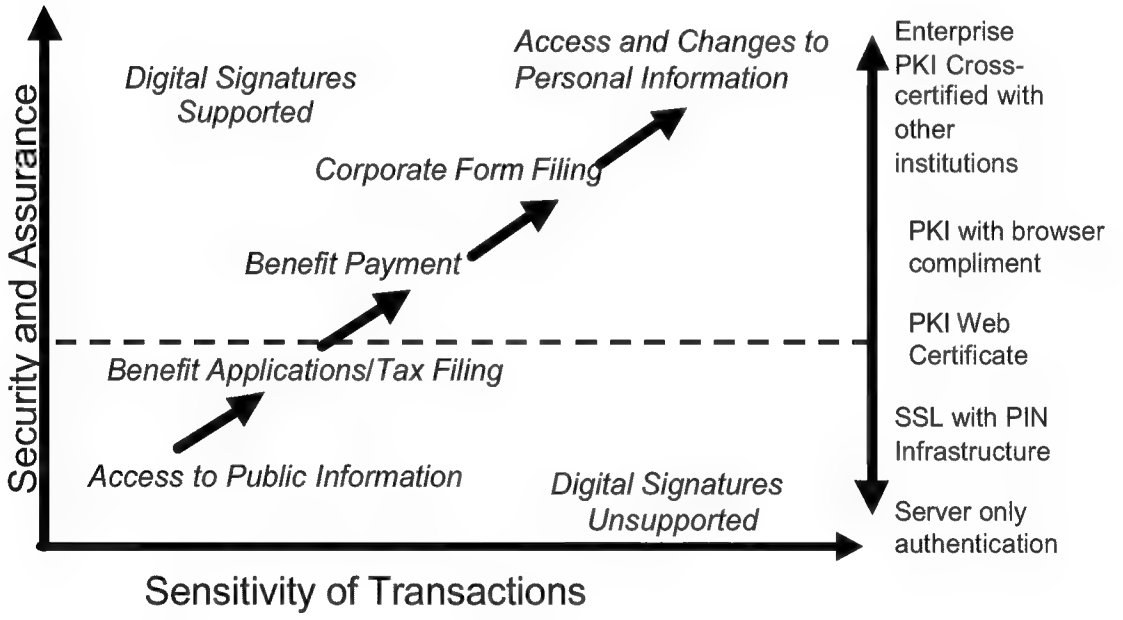


7.4.1. Balancing the Risk - The Need for a Range of Security Options

Clearly, some information and assets are significantly more critical than others. ***There is no "one size fits all" security solution***. Development of a security architecture therefore involves a range of risk management trade-offs. With regard to provision of government services on line, one approach is to define a set of business transactions with a corresponding range of security solutions. However, it is not enough simply to adopt a broad spectrum of incompatible and non-interoperable security solutions. These solutions should fit into an integrated security architecture, that also takes into account the management requirements associated with the selected security solutions.

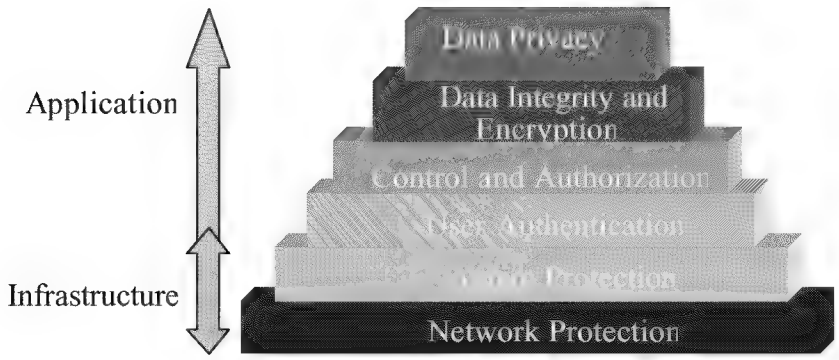
As an example, the following chart illustrates the possible range of security options suitable for user authentication in different types of Internet-based business transactions. Although this example is specific to authentication technologies, a similar continuum of options can be applied to most technical security safeguards.

Range of Security Options for Authentication



7.4.2. Technological Controls

The best method of securing a network or host is to use multiple security technologies together as part of a ***layered security architecture*** as depicted below. A layered security architecture is modular. Network and systems infrastructure layers support higher level applications. Each layer has its own security requirements and, in order to get complete coverage, all layers have to provide information protection measures.



Layered Security Architecture

Different security technologies have different strengths and weaknesses, but together they can create a reasonably strong barrier against most attackers. Understanding the strengths and weaknesses of the technologies is also necessary to develop appropriate security practises and procedures.

There are a wide variety of advanced security technologies such as Public Key Infrastructure (PKI), firewalls, virtual private networks, intrusion detection systems, operating system security, smart cards, digital signatures, and others. A layered security architecture takes advantage of a balanced set of these technologies, but also takes into account policies and procedures, risk management, incident handling, vulnerability analysis, and other essential activities. Since no combination of security technologies can be completely secure, governments must also be prepared to respond to successful attacks.

The following provides an overview of common security technologies:

(1) **Application Layer Security**. Application layer security provides ***end-to end or writer- to-reader security*** for transactions. Application layer security services protect application-specific information and transactions. Some specific application layer security services include authentication, transaction encryption and digital signatures, transaction logging and recovery mechanisms. Some security services – notably non-repudiation – can ***only*** be performed at the application layer. One of the principal problems is that application software often contains numerous vulnerabilities and, although multiple techniques can be applied to form a barrier, ultimately users must interface with the application.

(2) **Operating System Security**. The Operating System provides a barrier to ***protect the applications and data on a computer***. An Operating System has direct control over applications and provides security services to, and around, an application. Operating Systems can create a strong shell of security around the applications, provide secure communications among applications, limit penetrated applications from spreading their influence, and limit the leakage of critical information out of an application. Some examples of Operating System security features include trusted path, least privilege, non-discretionary access protection, and strong

authentication. However, some Operating Systems allow applications too much control and thus vulnerabilities in applications can lead to a complete compromise of the computer. Operating Systems themselves often have numerous vulnerabilities; nevertheless, much of the public continues to purchase Operating Systems known to be insecure.

(3) **Network Layer Security.** Network layer provides ***domain to domain*** security. Network layer security provides security services including access control, confidentiality, and integrity protection that all applications can use. A ***Virtual Private Network (VPN)*** is created using encryption to isolate the traffic between two communicating hosts from other traffic on the network. Since network layer security provides a barrier for all applications, it can reduce costs and reduce application integration problems. However, network layer security cannot perform "transactional" security services such as non-repudiation because the information contained in transactions is only understood at the application layer.

(4) **Firewalls.** Firewalls provide ***perimiter defence.*** As the term implies, a firewall restricts overall access from an untrusted environment (the Internet) to a friendly environment (the local network). Firewalls police network traffic that enters and leaves a network. A firewall may completely disallow some traffic or may perform some sort of verification on traffic. A well-configured firewall can block many known attacks and can prevent attacks by disallowing protocols that an attacker could use. By limiting access to host systems and services, firewalls provide a necessary line of perimeter defence. However, firewalls do not, in most environments, adequately reduce the risk for active content or transaction-oriented services. For example, firewalls do not typically have the ability to analyze downloaded Java applets. New transaction-based Internet services make these "perimeter" defences less effective and the boundaries between the internal and external environments "blur". A firewall controls broad access to all networks and resources that lie "inside" it. Once packets traverse the firewall and enter the internal network, the firewall cannot prevent access to or modification of internal resources. For Internet-based transaction systems, the security mechanisms must be able to provide or deny access to particular web pages, applications, and databases on the basis of individual user profiles and authentication. Firewalls are unable to provide such detailed security measures.

(5) **Public Key Infrastructure.** The PKI manages ***electronic identities and cryptographic keys.*** Since most security technologies today rely on encryption and digital signatures, a Public Key Infrastructure (PKI) is normally a fundamental part of a security architecture and is integral to the secure service delivery model. A PKI provides a mechanism to manage and ensure ***trust in electronic identities***, which is critical because almost all security services rely on identification and authentication. In addition, a PKI provides an infrastructure to ***support trusted interactions*** between the government and external partners, businesses, and citizens. A PKI is the only technology that can provide such an infrastructure. The PKI supports encryption and digital signature capabilities across a broad range of both application and network layer products to provide authentication, integrity,

confidentiality, and non-repudiation. A typical PKI integrates digital certificates, public-key cryptography and certificate authorities into a total, government-wide security architecture. It also encompasses the issuance of digital certificates to users and servers; end-user software; certificate directories; tools for managing, renewing and revoking certificates; and related services and support.

(6) **Authentication Technology.** This technology confirms the ***identity*** of users or administrators. Authentication technology is important because almost all other security mechanisms rely on it. "Simple" authentication refers to mechanisms such as passwords and PINs. "Stronger" authentication mechanisms include challenge-response schemes, one-time passwords, and cryptographic schemes such as digital signatures using X.509 certificates (PKI). Additional assurance can be obtained using so-called "two factor" authentication, in which the cryptographic technology is securely contained in a smart card or token.

(7) **Intrusion Detection**. Intrusion Detection Systems (IDSs) provide the ***security alarm system***. IDSs detect unauthorized use of, or attacks on, a computer or network. Given that it is not possible to prevent all potential attacks, IDSs are extremely valuable tools for detecting, analyzing and responding to attacks when they do occur. Using IDS to support so-called "active" information protection is becoming an important component of a security architecture. There are two basic types of IDSs: network-based and host-based. Network-based IDSs are effective tools that provide insight into network activities to detect and analyze attacks. Host-based IDSs are effective at detecting and analyzing attacks based on audit files of a specific host. IDSs are an emerging technology and do have limitations. IDSs normally detect attacks that have occurred, but cannot prevent attacks. They must therefore be used in conjunction with other forms of preventive security measures. In addition, they are normally only able to detect attacks that have previously identified "attack signatures" that have been analyzed by the IDS vendor.

(8) **Virus Detection Software**. These are also ***alarms*** specifically designed to detect viruses. Virus detection software monitors computers and detects malicious code. Virus detection software must monitor all points of entry. For example, virus checkers on e-mail servers that scan e-mail attachments should supplement virus checkers on hosts. Since new viruses are constantly being identified, virus detection software needs to be updated frequently. Despite frequent updates, it is possible that new fast-spreading viruses can infect a network before virus-detection manufacturers can release software updates. In addition, virus-detection software can only detect viruses that a vendor has previously identified and included in the software. Malicious software that is custom built for a specific attack will escape detection.

(9) **Vulnerability Scanners**. Vulnerability scanners are ***quality assurance tools*** to verify that systems are implemented correctly. Vulnerability scanners are programs that scan a network or hosts to detect vulnerabilities. Scanners use a large database of known vulnerabilities to probe computers to locate the vulnerable

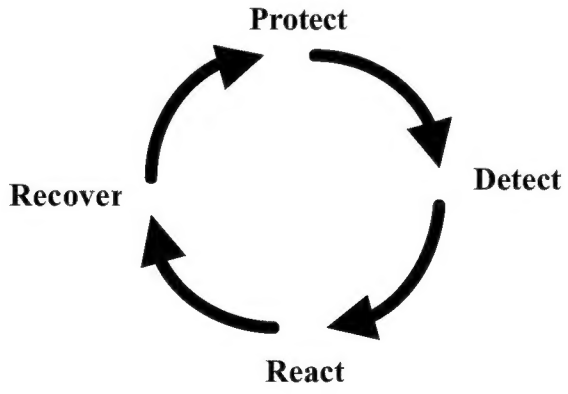
ones. They are effective at finding vulnerable hosts so that corrective action can be taken; however, they are limited to previously identified vulnerabilities.

(10) **Evaluations**. Evaluations provide ***assurance*** that the information system is secure. Most security managers depend almost exclusively on vendor information about the security of new software or systems. Given the potential implications of a security system failure, critical security solutions should undergo independent evaluation, testing, and validation. The Common Criteria is an internationally accepted standard for product or system evaluations that can increase the level of trust in a product or system. It should be noted that other processes, such as a Certification and Accreditation (C&A) process and the System Security Engineering Capability Maturity Model (SSE-CMM), also serve to increase the level of assurance in information systems.

7.5. Active Information Protection

Although a carefully implemented security architecture will reduce the risk, it cannot provide total security. In fact, our ability to safeguard information systems is not keeping pace with the increase in Internet threats, vulnerabilities, and attacks. Governments need to be able to react quickly and effectively when an incident does occur. In addition to the security measures discussed previously, security in a dynamic Internet environment requires an "active" operational component. Active information protection includes operational processes for ***protection, detection, response, and recovery***. These processes are typically supported by an Information Protection Center (IPC). An IPC allows an organization to react quickly to the dynamic nature of the threat and to response when an incident does occur.

Information Protection Cycle



The following is a brief discussion of the components of active information protection:

(1) **Protect**. This involves activities such as network mapping and asset identification, security posture assessment, security alerts and advisories, and provision of a central Information Protection repository. Network mapping is used to identify the electronic perimeter of a network. Security posture assessment uses appropriate tools to perform vulnerability assessments,

penetration testing, and audits. Security alerts and advisories consists of monitoring and publishing information on current security incident activities, vulnerabilities, the release of hacker tools, and new viruses/trojans etc obtained from public domain and trusted security sources. The Information Protection repository provides a trusted repository of security-related expertise and reference materials such as vulnerability databases, "best practices," and reference reports and guidance documents.

(2) **Detect**. This involves activities such as incident detection, reporting, and attack monitoring. Incident detection uses technologies such as Intrusion Detection Systems and other sensor and logging devices to detect and report anomalous behaviour. Intrusion Detection Systems require continuous monitoring to provide timely warning of incidents and attacks. Monitoring also requires both automated approaches and significant manual analysis. Once a potential attack is detected, tracing and monitoring is required to determine the severity and extent of the attack, gather evidence, contain the attack, determine the potential for escalation, coordinate responses to multiple distributed attacks, and determine the effectiveness of countermeasures.

(3) **React**. This involves incident handling, damage containment and control, and analysis of incident information. It requires a well-defined and managed process to deal with incidents in an organised and disciplined manner, including formal procedures and coordination with other Incident Response Teams. Damage containment and control is required to minimize both the effect of an attack and the exposures of interconnected networks by preventing propagation of the attack or malicious code. The response must preserve evidence and remnant files. Technical support is required to support incident response, including the analysis of logs and related activities.

(4) **Recover**. This process involves activities such as analysis of remnants and malicious code, re-activation, and recovery. Intrusions generally leave what are called *remnant files* that represent the "fingerprint" of the intruder. These are important evidence regarding the incident. Recovery requires a "quarantine" to contain the attack and preserve evidence, along with the procedures and tools necessary to rebuild systems. Critical systems may require immediate restoral which may involve a reduced level of service (e.g. fewer services, new procedural requirements, changes to interconnections, regression of applications or information to older versions). Finally, incidents must be reported and, if necessary, new security functionality implemented.

It is emphasized that a balanced approach is needed. An IPC will not be effective if the other safeguards described in this report are not in place. Similarly, it is difficult to ensure the safeguards are working effectively without some form of active information protection. In addition, effective Information Protection requires coordination and sharing of information due to the complex nature of the threats. This requires a structured cross-jurisdictional capability such as a national information protection coordination center.

8. CONCLUSION

Provision of government services over ***the Internet has become an imperative*** in the new Information Age. When governments use the Internet for service delivery, however, ***security and privacy*** are fundamental requirements. This report has provided an overview of the threats and vulnerabilities to government information systems in this environment and emphasizes the need for implementation of a sound information protection program to meet the security challenge. Although these threats can seem daunting, this report also provided an overview of the elements of an information protection program, which, if carefully implemented, ***can significantly reduce the risks*** which governments must address.

Much more work remains to be done. Particular emphasis is being placed on protecting Canada's critical infrastructures. The federal government recently established an interdepartmental Critical Infrastructure Protection Task Force to address this challenge. In addition, a national focus is required to develop national security infrastructures such as a national information protection coordination center and Public Key Infrastructure. These elements will require partnerships between governments and the private sector in order to achieve the ultimate goal of a secure national information infrastructure.

REFERENCES

---

[1] GAO/AIMD-98-68, Executive Guide, Information Security Management - Learning from Leading Organizations, May 1998

[2] The Report of the Special Senate Committee on Security and Intelligence, January 1999

[3] Testimony of Stephen Cross, Director Software Engineering Institute, Carnegie Mellon University, before the U.S. Congress, 23 February 2000

[4] Issues and trends: 2000 Computer Crime and Security Survey, Computer Security Institute, March 2000

[5] ICSA 1999 Infosecurity Year-in-Review, M.E. Kabay

[6] Internet Auditing Project, Liraz Siri, 11August, 1999

[7] Report on the Threats to Selected Government of Canada Internet Sites, prepared under contract for the Communications Security Establishment by Electronic Warfare Associates-Canada, 17 November 99

[8] Saskatchewan Government IT Security Workshop, conducted by CanCERT under contract to the Government of Saskatchewan, 14-15 March 14-15 2000

[9] Operation Caveat Lessons Learned Report, Communications Security Establishment, April 2000

[10] Information Security Management and Assurance: A Call to Action for Corporate Governance, Institute of Internal Auditors (IIA) under contract with the U.S. Critical Infrastructure Assurance Office, March 2000

[11] Fundamental Improvements Needed to Assure Security of Federal Operations, GAO/T-AIMD-00-7, Statement of Jack Brock Jr, General Accounting Office, 6 October 1999

[12] Operationally Critical Threat, Asset, and Vulnerability Evaluation Framework (OCTAVE) Framework, Version 1.0, Software Engineering Institute, Carnegie Mellon University, June 1999.

[13] Continuous Risk Management Guidebook, Software Engineering Institute, Carnegie Mellon University, 1996